

references of record, that the claims are not in compliance with 35 U.S.C. 112, second paragraph, and that various references owned by a common assignee impact on the patentability of the present invention. The undersigned will answer each of these assertions as best can be assessed from the office action.

However, the above-identified application was under appeal. If the Examiner persists in rejecting the claims, the undersigned requests that the appeal be reinstated.

Inventorship and U.S. Patent 6,226,619

The present application was filed on October 29, 1998 naming Mr. Coppersmith, Mr. Greengard, Mr. Tresser, and Mr. Wu as joint inventors. The undersigned confirms that these are the correct inventors for the present application.

U.S. Patent 6,226,619 was filed on the same date as the present application naming different inventors, some of which are in common with the inventors in the present application. U.S. Patent 6,226,619 claims different subject matter.

In view of the above, there is no confusion on the record about inventorship. Furthermore, because the inventions are different, it would be improper to lodge a rejection based on the judicially created doctrine of obviousness-type double patenting.

For clarity, and in response to the Examiner's question, all claims were commonly owned at the times the inventions were made. Therefore, there is no obligation to identify any invention dates for either the present application or U.S. Patent 6,226,619.

35 U.S.C. 102(e), 35 U.S.C. 103 and U.S. Patent 6,226,619

The present application has the same effective filing date as U.S. Patent 6,226,619. Therefore, U.S. patent 6,226,619 is not a valid reference against the present application under 35 U.S.C. 102 or 35 U.S.C. 103. See MPEP §706.02(f) where it indicates that one of the requirements to be a reference against another application is for the "effective filing dates" to be different. In this case, the effective

filing dates are not different.

35 U.S.C. 102(e) and U.S. Patent 6,069,955

U.S. Patent 6,069,955 to Coppersmith describes a system for protection against counterfeiting. This system employs private keys and public keys and was developed by the same inventive entity as the claimed invention. The effective filing date of U.S. Patent 6,069,955 is less than one year prior to the filing of the present application. As such, U.S. Patent 6,069,955 is not a valid reference against the claimed invention.

35 U.S.C. 103

As the Examiner should well know, an applicant is entitled to a patent unless “the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains” 35 U.S.C. §103(a). To render a claim obvious under 35 USC § 103(a), two requirements must be met. First, the cited references, when combined, must teach or suggest all the features of the claimed invention. Second, there must have been some teaching or suggestion in existence at the time the invention was made to combine the cited references in the manner claimed. Unless both of these requirements are satisfied, a claim cannot be regarded as being obvious over a combination of the cited references. See MPEP § 2143; *In re Rouffet*, 47 USPQ.2d 1453 (1998); and *In re Fine*, 5 USPQ.2d 1596 (Fed. Cir. 1988).

In this case, claims 1, 16 and 21 are independent claims.

Claim 1 of the patent application is drawn to a system for verifying authenticity of a manufactured product which includes an electronic tag that is attached to the product or its packaging which includes a memory that stores authentication information for the product in encrypted form, and a reader equipped with a decryption key for reading the authentication information in order to verify the

authenticity of the product.

Claim 16 is an independent method claim which recites the method by which the system of claim 1 is used. In particular, authentication information for a product is generated and encrypted using a private key, and the encrypted information is stored on an electronic tag that is attached to the product. The encrypted information is later read and decrypted using a public key to verify the product is authentic.

Claim 21 is an independent method claim drawn to detecting manufactured products in a parallel market. Claim 21 requires that routing information stored on the electronic tag is checked to see if it matches routing information of the point of sale so that it can be determined if the product is sold in a parallel market.

In the present invention, the manufacturer is in control of producing matching pairs of private keys and public keys, and the widespread availability of the public key does not compromise the security of the private key. In this way, the electronic tag system and method of this invention allows a verifying agent to be convinced that a tag is authentic without the tag revealing the authentication information. With reference to Figure 1, the manufacturer 101 generates a serial number or other information with generator 102 that is encrypted using private keys 103 and 104. A label is printed that is attached to the product and a smart card is produced which contains the encrypted information which is also associated with the product. Public keys 109 and 110 are generated by the manufacturer 101 which are then made available (e.g., over the Internet). Thus, the customer can verify the authenticity of the product by examining the physical label using public key 109 or can verify the hidden label using public key 110.

#### *The Prior Art*

None of the references of record have been analyzed by the Examiner in the office action in sufficient detail that one could ascertain from the references, alone or in combination, how or why the claimed invention might be obvious. In fact, a

Careful review of all of the references of record makes it clear that none of the references are precisely on point to any of the claims, and further, that even if one of ordinary skill in the art being in possession of all of the references, the claimed invention would not be obvious to them.

The 7/5/98 *Washington Post* article says no more than that smart cards can be used in conjunction with rail travel and for payment (debiting) of various fares. There is no mechanism for encrypting and decrypting information to verify authenticity of an article, which is the central focus of the claimed invention.

The Fuji-Kezai reference describes the use of a smart card with encrypted data. However, it can be seen that the article deals only with data storage and retrieval concepts. (No suggestion of a manufacturer generated private key-public key authentication system is made.)

The Washington Times article deals only with a smart card used as a fare card for debiting functions.

The Dialog Classic Web reference entitled "Report on Smart Cards" merely reports on the launch of various smart card debit cards.

The Dialog Classic Web reference entitled "Ramtron gets order..." merely reports that smart cards are being widely used in a variety of applications. These include data storage and debiting.

The newly cited Dialog Classic Web reference entitled "Liquor Marketing..." discusses Grey market goods and concerns over counterfeiting. It does not mention any verification technique similar to that described in present application. Furthermore, there is no routing information addressed similar to that set forth in claim 21.

The newly cited Dialog Classic Web reference entitled "Parallel lines..." is also directed to counterfeit products. This reference does not describe anything other than counterfeit imports being a problem. The reference does not mention any verification technique similar to that described in present application. Furthermore, there is no routing information addressed similar to that set forth in claim 21.

search →

The newly cited Capital Hill Hearing statement from the House Judiciary Committee discusses the problems of counterfeiters and discusses the practice of affixing fake codes to products. However, the report suggests no cheap and effective mechanism for thwarting such activity. If anything, the reference demonstrates that there is a need for the claimed invention, and that despite this need it was not obvious to anybody how to solve the problem.

The newly cited DialogClassic Web article entitled "Get Ready for the Jobs..." discusses new careers which will arise based on the wide spread use of computers and storage devices. It does not address product verification or identification of parallel market information.

The newly cited DialogClassic Web article entitled "D&G Taking a Bite Out of Bogus Goods" article discusses using invisible codes, holograms and other security measures to identify counterfeits and parallel market goods. This reference does not discuss a manufacturer controlled private key-public key verification system or method.

The newly cited DialogClassic Web article entitled "Smart Card Missionary GEMPLUS..." discusses the promising future of smart cards. It identifies data storage, security and other applications. However, there is no suggestion of a product authenticity verification methodology system or method.

The newly cited DialogClassic Web article entitled "GE Capital and GEMPLUS..." indicates the joint venture will make, among other products, electronic tags. There is no mention of how the electronic tags will be used or what information they will hold. The Examiner should note that smart cards have been widely used for security purposes whereby access to gated areas is provided or denied, etc. Also smart cards commonly hold identifying information or other data (e.g., medical records). However, the claimed invention is directed to a specific system and method whereby electronic tags are used in a particular way in conjunction with private key-public key encryption and decryption technology to verify product authenticity or routing information. None of this springs from the statement that "electronic tags"

*argue*

will be manufactured by the joint venture.

The newly cited DialogClassic Web article entitled "Leading Smart Card..." also mentions smartcards and electronic tags. But, like the GE Capital article noted above, the article does not show or suggest a system or method for verifying product authenticity or identifying a parallel market product by encrypted routing information.

The newly cited DialogClassic Web article entitled "The battle against counterfeiting" merely discusses the problems of fake products and parallel market sales. No authentication procedures or systems are mentioned.

The newly cited DialogClassic Web article entitled "Counterfeit goods samples provided..." merely discusses the need for the Customs office to provide trademark and copyright holders with unaltered counterfeit goods so that they might better identify their source or origin.

??  
None of the patents identified in the office action show or suggest the claimed invention, alone or in combination with any of the references of record.

U.S. Patent 6,078,888 to Johnson describes a cryptography security system which employs a smart card and a receiver-on-computer-system-in-a-car, as well as a transmitter associated with the key. No authentication of product authenticity is performed.

search

U.S. Patent 5,892,441 to Woolley merely describes a process for sensing electronic tags. It does not discuss or suggest encrypting information on a tag using a private key, and decrypting the information at a later time using a public key so as to verify product authenticity or routing information.

U.S. Patent 5,367,148 to Storch describes a counterfeit detection system which uses ID numbers. Storch does not employ a smart card with encrypted information using a private key that is later decrypted using a public key.

U.S. Patent 5,901,303 to Chew discloses a smart card system. The patent is directed to storage and access of data. The patent is not related to product authenticity verification.

U.S. Patent 5,164,988 to Matyas discloses a network security system in a

public key cryptosystem. This patent has nothing to do with smart cards or product authenticity verification.

U.S. Patent 5,971,435 to DiCesare et al. discloses a method for verifying the authenticity of an autograph. It does not employ a private key encrypted tag associated with a product, and does not contemplate or suggest using a public key decryption methodology to verify authenticity.

U.S. Patent 5,140,634 to Gouillou et al. describes a message authentication system and method. This patent does not relate in any way to product authenticity verification.

U.S. Patent 5,740,250 to Moh describes a public key system which can be applied to, among other things, smart card security. However, the Moh reference does not have anything to do with product authentication or routing authentication. Rather, Moh is only concerned with the security of the card itself, not a process or system whereby electronic smart card tags are used in a private key encryption and public key decryption procedure to verify the authenticity of the product.

U.S. Patent 4,463,250 describes an anticounterfeiting system which determines if a label on a product is authentic and has been read before. No smart card technology is implicated.

U.S. Patent 5,721,781 to Deo describes a smart card transaction system where debiting is employed. Deo is unrelated to product authenticity verification.

U.S. Patent 5,687,236 to Moskowitz is related to a steganographic method. In this invention, "additional information" is encoded in a stream of digitized information and is later decoded. This method has nothing to do with the claimed invention whereby product authenticity is verified.

U.S. Patent 4,864,110 to Guillou describes an electronic payment process using a smart card. The reference has nothing to do with product authenticity verification.

U.S. Patent 4,995,082 to Schnorr describes an electronic signature system. This system is unrelated to product authenticity verification.

In view of the above, the Examiner should reconsider and allow all claims pending in this application at the earliest possible date.

Respectfully submitted,



Michael E. Whitham  
Reg. No. 32,635



30743

PATENT TRADEMARK OFFICE